Amendments to the Claims

1. (currently amended) A versatile customizable security and filtering software embedded upon a computer-readable medium, the software capable of being ~~that can be~~ installed on a computer and be used by a remote user who obtains anonymity on a global telecommunications network or by a local user, the software comprising:

(a) an administrative module that a user interacts with for creating user accounts and configuring those user accounts, and for configuring automated services,

the administrative module for accepting user inputs for configuration settings for inbound communications and for outbound communications, and having list maintenance functions including list editing, ~~list deleting, searching of lists, saving of lists, proxy chaining routing, adding and deleting users, interchanging lists and importing and exporting lists,~~

said administrative module for configuring a range of access levels and being capable of creating ~~three types of~~ user accounts that have unique user names and passwords for each user account including an administrator account that is self-configuring and that controls automated services and selects for each account hard filtering or soft filtering, regular accounts with administrative privileges other than the privilege to create additional accounts, view information on any other accounts or configure automated services and regular accounts without administrative privileges and in addition a fourth type of user account namely one anonymous guest user account to be used in a manual launch of the software by general users who have no system-based user name or password,

the administrative module for storing as encrypted files on hardware memory the

alert to authorized recipients regarding the disapproved request, wherein, for requests that are terminated and re-rerouted, inbound communications are arranged so that an actual location of a highly sensitive resource is located in an unpublished location that is a replacement location to which requests rejected by the application server are rerouted, wherein clients of approved users are listed in the application server in the unfriendly inbound list and are sent by the application server to the replacement location, and wherein clients of unapproved users are not listed in the unfriendly inbound list and have their request sent to a published address that contains harmless information.

~~and~~

~~(ii) a content filtering engine capable of performing content filtering including checking a content of a requested document against a friendly content inbound list, an unfriendly content inbound list, and a content exception list taken from the encrypted files, the friendly content inbound list, the unfriendly content inbound list, only one of the friendly content inbound list and the unfriendly content inbound list being active at any given time, and the content exception list being uniquely configured by each user, and then for hard filtering against the unfriendly content inbound list either passing the requested document if the content of the requested document is not on the unfriendly content inbound list or unless overruled by the content exception list rejecting the requested document if the content of the requested document is on the unfriendly content inbound list and for hard filtering against the friendly content inbound list either unless overruled by the content exception list passing the requested document if the content of the requested document is on the friendly content inbound list or rejecting the~~